January 2021 Phishing Scenario Results: DocuSign Credential Theft Scam

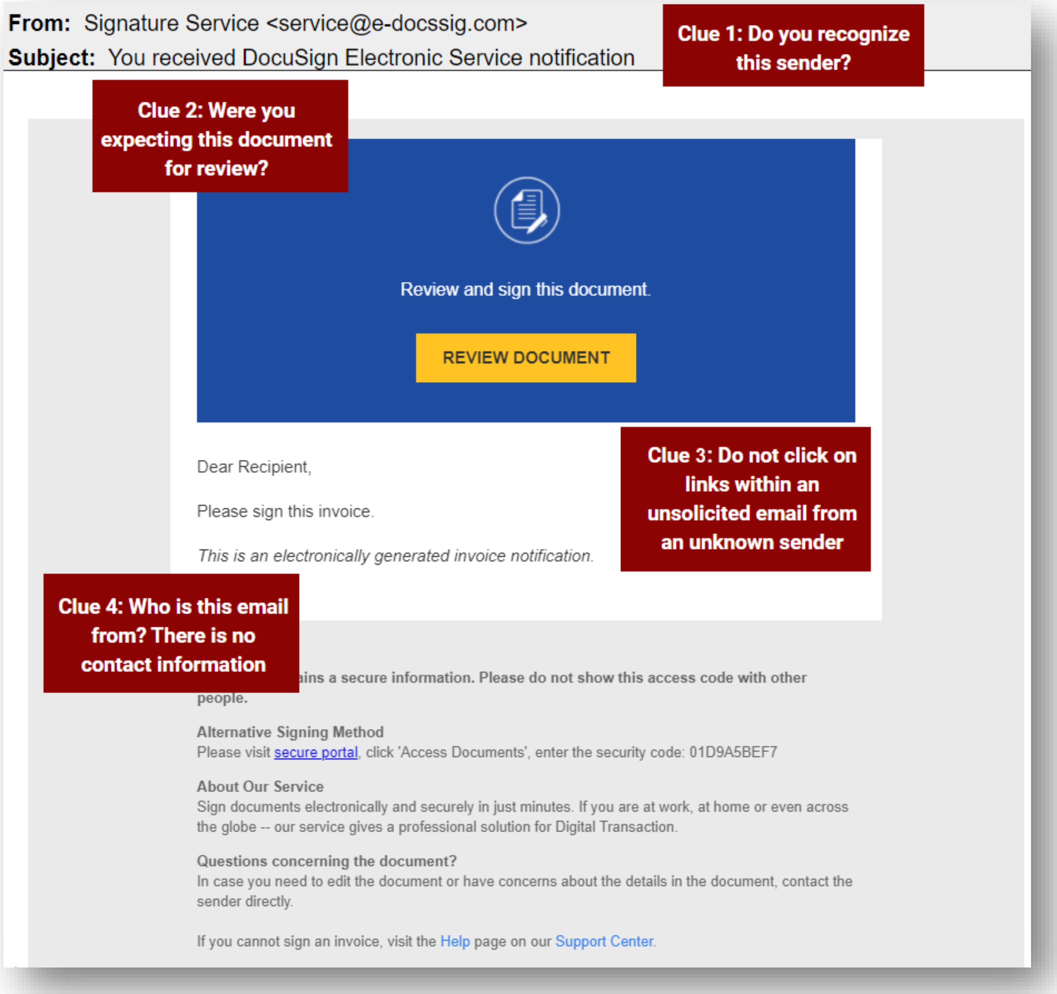
The Office of Information Technology's (OIT) first phishing scenario of the new year is an old threat – a DocuSign email notification inviting you to review and sign a document. Bad actors frequently impersonate trusted brands, like DocuSign, to lure you in. Upon clicking the link, a login prompt is displayed. This is a credential harvesting phishing attempt to capture your login credentials.

915 employees reported the phishing email to the Phishtrap! Reporting is the preferred action as it provides IT Security the email threat intel it needs to respond.

232 employees clicked the link, but did not enter credentials.

140 employees clicked the link AND entered their MyMC credentials. In a real phishing email, this would provide an attacker complete access to your MyMC and Office 365 accounts!

OIT's phishing awareness program is designed to educate employees about potential email threats AND to encourage **reporting of suspicious emails**. Please take the time to review the clues in the DocuSign scenario:



From: Signature Service <service@e-docssig.com>
Subject: You received DocuSign Electronic Service notification

Clue 1: Do you recognize this sender?

Clue 2: Were you expecting this document for review?

Dear Recipient,

Please sign this invoice.

This is an electronically generated invoice notification.

Clue 3: Do not click on links within an unsolicited email from an unknown sender

Clue 4: Who is this email from? There is no contact information

ains a secure information. Please do not show this access code with other people.

Alternative Signing Method
Please visit secure portal, click 'Access Documents', enter the security code: 01D9A5BEF7

About Our Service
Sign documents electronically and securely in just minutes. If you are at work, at home or even across the globe -- our service gives a professional solution for Digital Transaction.

Questions concerning the document?
In case you need to edit the document or have concerns about the details in the document, contact the sender directly.

If you cannot sign an invoice, visit the Help page on our Support Center.

What should you do if you suspect an email may be a phishing attempt?

Report
Phishing
MC

Let IT Security analyze the email for you - **REPORT** the email! Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed in MC Learns through Workday.

Below are some common clues to look for in identifying a suspicious email:

- Be wary of emails from unknown senders. PERIOD.
- If you are expecting emails containing shared documents or requiring a signature – find out who the sender is, the domain of the sending address, what product they use to share the document, etc. For DocuSign, access your documents directly from DocuSign's website, https://www.docusign.com
- Check your emotions. Do not be curious and investigate the link – REPORT the email.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.
- Another red flag - the message is overly generic, the request is outside of your scope of responsibility, and/or the action requested is not typical of a current business process.
- Visit IT Security's Phishing Alerts web page to view the latest threats – this month's feature is on Stimulus Phishing Scams.

If you have any questions or concerns regarding this process, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT’s web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology